MARCH 2020
networkingplus.co.uk

NETWORKING+

Performance and agility

How to improve it with automation and AIOps

Vijay Kurkal, Resolve, p7

A backbone for success

Helping businesses sharpen that competitive edge

Paul Ruelas, GTT, p13

Meet Matthew Pincus

Find out which UK law he'dlike to change

Matthew Pincus, Halo Tech Group, p15

COVID-19 compels UK to embrace remote working

Companies across the UK are taking fresh action in hopes of preventing employees from getting exposed to Covid-19, by restricting travel, encouraging remote working and using tools such as video conferencing.

The move came after prime minister Boris Johnson said employees should work from home where possible, in a bid to navigating coronavirus, which causes the new illness.

Using video services such as Zoom and Skype have become the norm for remote workers in this unprecedented time and some have questioned whether company networks and home broadband connections will be able to handle the increased traffic.

"The possibility of the UK having to remotely work over the next few months has led to questions about the ability of ISPs to handle the additional workload of employees working from their homes," said Andrew Glover, chair of the Internet Services Providers' Association (ISPA). "ISPs are ready to handle any potential extra bandwidth and consistently assess the demands that are being put on their networks. Businesses and companies will need to ensure that their own systems, e.g. their server setup, support a potentially significant increase in remote connections to accommodate the potential increase in traffic from their employees."

Simon Moxon, founder and chief executive officer (CEO) at business video conferencing service Meetupcall, told *Networking+* that a typical ADSL broadband connection should be sufficient for most work, such as email and web-based apps but there could be problems when it comes to high resolution photos or embedded video.

"There may be challenges for regular home broadband when it comes to video conferences, especially if the connection is being shared, or everybody else on the exchange is working from home too," he said. "In this instance, a conference call service that supports regular telephone dial-in should be considered to ensure those important meetings can go ahead without disruption. Providing the organisation has a good conference call service in place that provides multiple joining options, this shouldn't be too much of a challenge."

Shashi Kiran, chief marketing officer at cloud-first WAN company and end-to-end managed SD-WAN provider Aryaka, added: "An unprecedented number of employees are working remotely, something businesses are not prepared for. Conference and video calls are paramount in order to get their work done as usual. With unforeseen amounts of people dialling in from home, increased bandwidth traffic will inevitably follow. VPN systems are already flooded and will soon become overloaded.

continued on page 2

ROUNDTABLE: Hacking as a service?
P8-9

COVID-19 wreaks havoc for businesses

Continued from page 1

Mike Smith, managing director, Virgin Media Business said remote working is not just about ensuring your employees can access their emails from anywhere, "it's actually about giving your people the freedom to take their office with them" – enabling them to work quickly, securely and flexibly. "Achieving this is easier than before," he said. "Employees can now collaborate across different apps from home or wherever they choose to work – with a vast choice of enterprise-grade software, from video-streaming to project management – and this is creating a more dynamic, fluid working culture."

However, leadership trainer Hira Ali, who is also the author of Her Way to the Top: A Guide to Smashing the Glass Ceiling, said "despite the alarming rise in coronavirus cases", only a few organisations are taking steps to go online. "The use of platforms such as Zoom, Skype, Microsoft team and Facebook Workplace provides more flexibility, convenience and safety than physical spaces, since interactions are online and can be planned on your schedule," she added. "Companies can easily leverage technology to make it easy, accessible and safe for employees to work from home. Why haven't many opted for this already? Why hasn't there been a government mandate to work from home?"

Meanwhile, Johnson has bowed to public pressure to follow other world leaders and order schools across the country to lock their gates indefinitely. Teachers have started remote teaching pupils from home via video links and other distance learning tools. ■

Mobile UK's 'big four' sign £1bn rural network agreement

Mobile UK's four members, EE, O2, Three and Vodafone signed an unprecedented £1bn agreement to eliminate signal dead zones in remote areas.

The Shared Rural Network (SRN) will transform mobile coverage, countrywide and the programme will make 4G mobile broadband available to 95% of the UK and Mobile UK's members expect this will extend mobile coverage to an additional 280,000 premises and for people in cars on an additional 16,000km of the UK's roads, boosting productivity and investment in rural areas.

The project consists of MNOs investing to extend their coverage by upgrading their existing networks, working together on shared infrastructure and building new sites, with new government-funded masts being built to target areas with no mobile coverage from any operator.

This deal will also lead to increases in some areas by more than a third, with the biggest coverage improvements in rural parts of Scotland, Northern Ireland and Wales.

All four operators' individual networks will cover 90% of the UK, enabling rural businesses and communities to thrive.

"The Shared Rural Network partnership between the mobile operators and the Government is unprecedented in both its scope and its ambition," said Hamish MacLeod, director at Mobile UK. "Mobile UK looks forward to supporting the delivery of the programme in the coming years."

The quartet signed the deal with the secretary of state for digital, culture, media and sport, Oliver Dowden.

Dave Dyson, chief executive of mobile operator Three, said the deal was "a game-changer for the country". Vodafone chief executive Nick Jeffery added that it was "unmatched anywhere in the world".

The deal hit a snag earlier this year when other operators objected to the proposed cost of using BT-owned EE's equipment.

BT argued that its costs were fair based on how much it had invested over the years. ■

The project consists of MNOs investing to extend their coverage by upgrading their existing networks, working together on shared infrastructure and building new sites, with new government-funded masts being built to target areas with no mobile coverage from any operator

Warrington Council picks Pulse Secure to streamline secure access

Pulse Secure, the software-defined secure access solution vendor, has delivered a project at Warrington Borough Council (WBC), "designed to help deliver taxpayer value" and workforce flexibility through secure network access.

The council's Juniper VPN technology and RSA two factor authentication were ready for replacement, so the council put out a tender inviting vendors to propose new technology to deliver secure, selective access to its network for third party associates. It required a secure access platform that could initially support 100 licenses, with the potential to scale to meet changing demand while offering easy ongoing management.

WBC tested the proposed solution before selecting Pulse Secure "as the best fit" for its needs with DXC, a Pulse Secure Elite partner selected as the solution provider including a three-year contract with built-in software and service support.

The DXC team transitioned the council's network from Juniper SAs to Pulse PSAs in a two-day, on-site implementation project "with minimal interruption" to user services. Now, the council said, it can provide reliable and secure VPN access for its entire direct and indirect workforce, making remote and mobile working easier.

"[I was] really impressed with how DXC were able to implement our remote access solution, no impact to our customers, and no complaints either," said David Gallear, technical lead (network), resources and strategic commissioning directorate at Warrington Borough Council. ■

The DXC team transitioned the council's network from Juniper SAs to Pulse PSAs in a two-day, on-site implementation project "with minimal interruption" to services

EDITORIAL:
Editor: Robert Shepherd
roberts@kadiumpublishing.com
Designer: Sean McNamara
seanm@kadiumpublishing.com
Contributors: Gerry Moynihan, Paul Liptrot, Vijay Kurkal, Paul Ruelas, Mathew Pincus

ADVERTISING & PRODUCTION:
Sales: Kathy Moynihan
kathym@kadiumpublishing.com
Production: Suzanne Thomas
suzannet@kadiumpublishing.com
Publishing director: Kathy Moynihan
kathym@kadiumpublishing.com

Networking+ is published monthly by:
Kadium Ltd, Unit 2, 1 Annett Road, Walton-on-Thames, Surrey, KT12 2JR
Tel: +44 (0) 1932 886 537

Printed in England by The Magazine Printing Company

ISSN: 2052-7373

East Anglia constabularies join forces to buy SC21 TETRA radios following successful trial

Norfolk and Suffolk Constabularies have acquired some 4,000 Sepura SC21 TETRA radios in a joint force investment, equipping their officers with powerful, compact critical communication devices.

The move followed a thorough trial by both forces, from which users gave the SC21 their enthusiastic approval, plus a comprehensive business case analysis, covering support, pricing and evolution of the product.

Sepura's SC21 is a compact version of Sepura's SC20 radio, combining high levels of robustness and functionality without compromising on performance.

Users on the trial lauded the SC21 in particular for its rich, clear audio, allowing clear communication even in noisy environments, as well as the compact design which takes up a minimum of space on an officer's uniform.

Officers also highlighted the excellent battery life and robust design of the radio and said that the intelligent user interface made it quick and easy to perform primary functions.

"Good communications is fundamental to our policing service and the SC21 will provide us with the support we need to give the best policing service we can to our communities," said assistant chief constable Steve Mattin, joint protective services lead.

David Woods, joint ICT airwave specialist for Norfolk and Suffolk Constabularies, was responsible for leading the trial and evaluation. "After considering the options available to us it was clear that Sepura's SC21 was the unanimous choice of both our front line officers and our operations teams," he said.

The SC21 is part of Sepura's SC Series of radios, featuring hand portable and mobile radios, supplemented by powerful applications and flexible accessories to support public safety officers to communicate efficiently. Sepura is the leading supplier to UK police forces as well as many other police forces in Europe and worldwide. ■

Users on the trial lauded the SC21 in particular for its rich, clear audio, allowing clear communication even in noisy environments, as well as the compact design which takes up a minimum of space on an officer's uniform.

Jubilee line 4G up and running in TfL planned trial

Transport for London's (TfL) planned trial with O2, Vodafone, Three UK and EE of a new 4G mobile (mobile broadband) network along the Jubilee Line has gone live.

Initially, this trial only covers the eastern section – platforms and tube trains in tunnels between Canning Town and Westminster stations – but the plan is to cover all platforms and tunnels on the whole of the line by the end of 2020.

The TfL project was first officially announced in July 2019 and ultimately aims to make 4G services available across the whole of their London Underground network by the "mid-2020s".

It will allow passengers to make phone calls, check for the latest travel information, catch up on social media, watch a video and read their emails or the latest news "uninterrupted" during their journeys. Ticket halls and corridors within stations are also covered by the pilot, except for London Bridge and Waterloo stations where the signal will just be available on the Jubilee line platforms.

"We're proud to be working with TfL and other mobile network operators to bring connectivity to where our customers need it most and we are excited to see the future potential of this project as it expands across the tube network," said Derek McManus, chief operating officer of O2.

David Dyson, Three UK's outgoing CEO added: "Every year, the average London commuter spends two weeks on the tube travelling to and from work, so there's a huge opportunity for us to help people reclaim that valuable time."

The trial was announced by TfL last July and went live March 17 2020. ■

FROM THE COVER

Feel the heat: putting liquid cooling front and centre in the data centre

Higher density chips are on the way. Liquid-cooled IT equipment is not new. It's been around for decades but recently has gained interest for more mainstream data centre applications. We tend to hear about it for niche solutions – such as for high-performance computing (HPC) and gaming. But today, there are some key trends and drivers that make it an appealing solution for the more mainstream IT audience. While data centre and edge environments today are primarily air-cooled, we are seeing a growing interest and value in the adoption of liquid cooling. The applications of cloud, IoT, AI, and edge are driving the continuous increase of chip and rack power density. There's also a continued focus on energy efficiency and cost. For many applications, liquid cooling is the optimal cooling solution. Today, air and liquid cooling options exist but many work harder, not smarter. Enter chassis-based immersive liquid cooling to solve the server chaos with the potential to optimise operations, efficiency, and cost.

Compared with conventional air cooling, liquid cooling provides benefits for data centre owners such as higher energy efficiency, smaller footprint, lower TCO, enhanced server reliability, lower noise, etc. However, liquid cooling also has some drawbacks such as higher investment, retrofit or redesign of servers, new data centre operation and maintenance skills required, etc

Join our webinar and find out how data centre owners can make an informed decision on whether liquid cooling has advantages for their application. This webinar session will focus on the major liquid cooling methodologies, the tradeoffs they bring in different environments and how Schneider Electric is leading an eco-system to create viable, commercial liquid-cooled systems that offer up to 15% lower CapEx and up to 30% energy reduction.

Register to attend.

ProLabs launches high-density transceivers

ProLabs has expanded its next generation 400G network capabilities with the launch of its new transceiver solutions to address rising network capacity demands. The company said that increasing 5G traffic is placing pressure on network operators to upgrade their current infrastructure. To address these challenges and meet the capacity demands, ProLabs latest transceiver – the QSFP28-DD 2x 100G – enables operators to increase port-density, solve interoperability issues between current and future infrastructure and minimise infrastructure investments. "For network operators to excel in a competitive market, it is imperative to deliver high-quality, high-capacity network connectivity in line with growing customer expectations," said Patrick Beard, chief technology officer at ProLabs.

Employees working from home targeted

Online scammers are using email phishing schemes in an attempt to profit on people's confusion and fear surrounding COVID-19, by targeting employees working from home. Hackers are leveraging the panic to transmit malware and break into computer networks, according to research from several cybersecurity firms. Hackers have sent phishing messages posing as the NHS, the World Health Organisation and health agencies from specific countries, purporting to offer information on the coronavirus disease, according to the firms. In some instances, the phishing emails appear to have been sent by hackers supported by US adversaries.

NHS Digital opts for Egress Protect

NHS Digital has chosen the Egress Protect solution to be integrated into NHSmail, considered to be the largest closed secure email network in the UK. The solution, which is aimed at offering improved protection and better user experience, is offered by human layer email security provider Egress. NHSmail is used daily by up to 1.5 million healthcare staff in the UK. The secure email service was approved by the Department of Health and Social Care for sharing sensitive information. Its function is for sending sensitive emails, which are encrypted, to non-secure email addresses.

Digital Realty opens data centre in Dublin

Digital Realty a global provider of colocation and interconnection solutions, has opened its Clonshaugh data centre, the latest facility in its portfolio of data centres in Dublin, Ireland. It represents a €70m investment and follows the company's previous €200m investment in the Dublin data centre market, culminating in the opening of its Profile Park campus last May 2019. The new Clonshaugh facility supports the further growth of Dublin's technology ecosystem. It is predicted to experience a multibillion-euro technology boom over the next decade, according to a study commissioned by Digital Realty and conducted by Development Economics, an economic consultancy providing robust research for clients ranging from Barclays to Facebook.

Nowcomm secures two new cybersecurity partnerships

Networking, collaboration and security technology specialist Nowcomm has formed partnerships with AT&T Cybersecurity, previously AlienVault and human cyber risk management platform Cybsafe. Through its partnership with AT&T Cybersecurity, Nowcomm will provide customers with access to an open source security information and event management system that simplifies the management of compliance and security, with a unified platform for all security monitoring and threat response. Meanwhile, Cybsafe's risk management platform will enable Nowcomm customers to improve the cybersecurity behaviours of their staff, by measuring current attitudes, developing metrics for cyber risk decisions, and identifying the most relevant areas for education and development.

Virtus announces go live dates

London data centre company Virtus Data Centres has completed the construction of its new London6 and London10 data centres in Stockley Park and Slough, which will open for business in early Q2 2020. These new facilities boost the company's total live London portfolio to 97MW, providing 23MW over more than 10,000 sq mt of technical space. London10 is Virtus' third data centre on the Slough Trading Estate.

University of Hertfordshire and Goonhilly in UK mapping data breakthrough

The University of Hertfordshire said its technology tie-up with the Goonhilly Earth Station in Cornwall will create business opportunities for enterprises and the agricultural industry by producing better-quality mapping data about the UK. It said that accessing Goonhilly's artificial intelligence (AI) and deep learning platforms has enabled it to create a service that will provide access to satellite mapping data of the UK that is free from cloud cover for the first time. It relies on the use of satellite radar imaging, which can penetrate clouds, to produce detailed images of the planet's surface regularly.

Jurassic Fibre gives deployment update

Full fibre UK ISP Jurassic Fibre, has issued an update on its progress and to announce the next set of deployment locations in the south west. The provider, which is currently being funded by an investment of £250m from Fern Trading Limited over the next five years, hopes to eventually reach as many as 350,000 enterprises and homes across Dorset, Devon and Somerset in England. Additional support is being provided by Tata Consultancy Services (software solution), Hydrotech Water Services UK, Swcomms and Barden Network Engineering (BNE). Jurassic Fibre has already connected its first business customer – luxury hotel Lympstone Manor.

White Horse chooses Altaro VM Backup

The White Horse Federation, a multi-academy trust, has selected Altaro VM Backup to back up data at over 32 primary and secondary schools across Oxfordshire, Wiltshire, Gloucestershire and Swindon. Its 23-strong IT team was becoming increasingly distracted by backup issues, time-consuming logistics and the need to physically move backups from one location to another. "Many hours were wasted dealing with distracting backup issues, cumbersome in nature, or physically co-ordinating backups between schools," said Mark Weller, White Horse's IT director and data protection officer."

Word on the web...

Social housing associations are constantly under increasing pressure to adapt to an ever-changing world. Nick Sacke, head of IoT and products at Comms365, explains the ways in which IoT can be used to create smarter and safer environments...

To read this and other opinions from industry luminaries, visit www.networkingplus.co.uk

sepura

Join Sepura and be a world leader.

Think of any emergency responder – police, fire, ambulance, motorway recovery, air ambulance and many more. You may well have come into contact with some of these organisations yourself.

All of these users will be wearing a critical communication radio device forming the crucial link between field operatives and the control room. Responders depend on these devices to communicate, keep in touch and automatically update the control room of their location, status and activity.

In the UK, the majority mission critical devices are provided by Sepura, developed and designed in our headquarters in Cambridge.

Engineers at Sepura play a key role in developing new products for our customers:

- Intuitive radios with powerful functionality
- Software to integrate with existing systems and expend the radio's capability
- User-friendly features to make the devices simple to use in complex or dangerous situations
- Conforming to strict international standards, protecting against dirt, water, dust and rain ingress

We are a world leader in our established technology, and we're investing heavily in developing the next generation of digital radio products and services as we shape the future of mission-critical communications.

We are looking for the best new engineers in the market to join us on our journey. To find out more about our current vacancies, visit www.sepura.com.

SEPURA CUSTOMERS INCLUDE:

NORWEGIAN POLICE

EAST ANGLIAN AIR AMBULANCE

HIGHWAYS ENGLAND

METROPOLITAN POLICE SERVICE

SHELL, SINGAPORE

9000 Cambridge Research Park
Beach Drive
Waterbeach
CB25 9TL
www.sepura.com

Human errors when emailing: break the cycle

Rick Goud, CEO & co-founder of ZIVVER takes a look at data leaks and how email could be playing a massive part

Research shows that employees spend an average of two and a half hours per day working on emails. Its ease of use and flexibility contribute to its popularity. Email is, however, risky as well, as shown by latest figures from the Information Commissioner's Office (ICO), which revealed that, of the 81% of data leaks caused accidentally by employees, 43% were due to misaddressed emails.

Other mistakes included adding the wrong attachment, or an attachment with unintended sensitive information. Or exposing recipient details by selecting the 'To' or 'Cc' email fields, when 'Bcc' should have been used.

Even though unintentional, such information-sharing errors still need to be addressed, in order to comply with legislation including the EU's GDPR (which continues to apply to all UK organisations, at least during the Brexit transition period).

So what can be done, to combat this type of 'insider threat'? Human error will likely never be completely eliminated, but, today, there are modern solutions available to help significantly reduce the chance of mistakes by giving employees feedback, on the spot, when working within their favourite tools. When sending emails or file transfers, for example. Such solutions use sophisticated methods to analyse patterns and algorithms, which help detect anomalies.

In a similar vein, the New Year's Honours List data leak – which was caused by human error - might have been prevented if some form of quality assurance had been used, to check that the content did not inadvertently contain any sensitive information before being published. Unfortunately it does not seem that any such measure was taken and the error was only discovered soon after the content was published, by which time it was too late.

To help IT and network managers minimise the number – and impact – of human error data leaks by staff, they could start by going through the following checklist, in conjunction with their trusted IT security provider:

- Increase employee awareness of how errors happen and the consequent implications: This has been named as one of the most important measures in GDPR, and similar legislation, and is the key to targeting the source of most data leaks: people inside the organisation!
- Prevent misaddressed emails: The number one cause of data leaks.
- Prevent unintended sharing of sensitive data: This umbrella category accounts for 81% of all UK data leaks.
- Prevent improper use of the 'Bcc' field when emailing: The ICO's most recent data security incident trends report has 'Failure to use Bcc' as a separately listed cause, due to its frequent occurrence and potential impact.
- Protect data from unauthorised access: The ultimate goal of all legislation related to privacy and protection.
- Apply data retention policies: Also a specific measure that is a key component in legislation such as GDPR.
- Guarantee message encryption: Email encryption is opportunistic, meaning it tries to deliver an email encrypted, and – if that is not possible - it will deliver the message unencrypted. Having guaranteed encryption is important for compliance to GDPR and HIPAA, for example.
- Limit the impact of data leaks: GDPR-like legislation requires organisations to have measures in place to safeguard against data leaks, as well as the capacity to mitigate potential damage when they do occur.
- Identify risks: The ability to have insight on how to improve data protection, which is essential for enhancing security standards and compliance.
- Measure the effects of measures: Improving security is about applying measures and assessing their effectiveness, always with an eye on how things could be better.

Organisations can achieve many aspects of the above by increasing their outbound email security efforts and defending against unauthorised access via two-factor authentication. If done in a way that is user-friendly, while also being simple to implement and maintain, organisations can unlock business value in areas including:

- Increased productivity by using email instead of fax, snail mail or USB sticks.
- Cost savings generated by a reduction in the use of snail mail, USB sticks or couriers.
- Reduced need for costly and ineffective customer portals.
- Savings on the labour costs of manually copying information to a source system.
- Strengthening the brand (adding a company logo to each secure message that is sent, for example).

With an expected yearly growth of more than 4%, email is, and will remain - for at least the next decade - the most important form of communication by organisations.

Safeguarding against human error when emailing is, therefore, poised to play a growing role across organisations of all sizes. This will be a result of increased general awareness of the top data breach drivers, while the corresponding fines for violations of data protection legislation become commonplace.

Rick Goud, chief executive officer & co-founder of ZIVVER

Improving network performance and agility with automation and AIOps

Vijay Kurkal, CEO, Resolve

In today's digital world, a business' success is inextricably tied to its ability to meet customer demands and rising expectations for quality, performance, responsiveness, and innovation. Digital transformation is no longer an optional add-on to help an organisation stand out in a saturated market. It is a necessity for businesses hoping to keep up with fierce competition.

In response to the hyper-competitive business climate, the pressure to quickly implement a new breed of digital services and workstreams has added further complexity and risk to an already challenging IT environment. The network required to adequately support this complexity while meeting customer expectations is unfortunately a distant reality for many enterprises.

Network professionals are fully aware of this conundrum, but too often their days are consumed by monotonous, low-value tasks and the fight to keep the network running smoothly. They simply don't have the time required for innovative thinking to drive digital transformation initiatives and to implement more effective technologies that can change the equation. In fact, a recent Gartner study found that two out of three digital transformation projects fail to achieve the desired outcome. However, this doesn't have to be the case. With new technologies like AIOps and automation, IT leaders can manage and mitigate challenges while delivering next-generation networks.

Today's networks are complex, vast environments. When things go wrong, it can be difficult to find the root cause as a single issue wreaks havoc throughout the ecosystem. Meanwhile, the myriad of network monitoring tools intended to keep things up and running have ironically created new challenges. A recent study by Enterprise Management Associates found that almost 25 percent of large enterprises have eight or more network performance monitoring (NPM) tools installed, with some implementing as many as 25. All these monitoring tools mean that network professionals are faced with multiple data sources when troubleshooting. They also contend with thousands of alarms every day – most of which are false positives – making it hard to see the wood through the trees and identify true events that need attention.

AIOps, or artificial intelligence for IT operations, cuts through the noise by applying machine learning to aggregate, analyse, and contextualise immense amounts of data from a wide variety of sources, including all of those monitoring tools. Right out of the gates, AIOps offers a single pane of glass into the network environment by bringing data together in one place to facilitate analysis and eliminate the swivel-chair interface.

Additionally, AIOps tools perform advanced event correlation and reduce alarm noise, highlighting real problems and intelligently grouping events, so Network Operations (NetOps) teams can take action. Further accelerating mean time to resolution (MTTR), these solutions use advanced analytics algorithms to pinpoint the root cause of network outages, eliminating the need for costly (and painful) IT war rooms, instead rallying only those resources required to fix the underlying issue behind all those alarms.

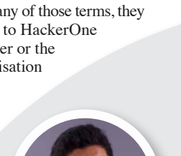
AIOps solutions also offer auto-discovery and dependency mapping capabilities that deliver powerful visibility into network devices and their dynamic relationships with business-critical applications. This enables NetOps teams to quickly evaluate the business impact of network device outages and to identify which business applications are at risk. Furthermore, infrastructure maps make it easy to visualise the root cause of issues within complex, hybrid environments. When an issue inevitably occurs, IT staff can spend less time hunting for the cause and move right to action while notifying business owners.

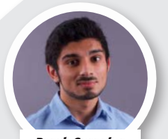
The ultimate potential of AIOps lies in its powerful predictive analytics. Once fully implemented, NetOps teams can rest assured that AI and ML are hard at work proactively identifying problems in the making, so they can be addressed before they impact end users, and in doing so, improving overall performance and customer experience. Insights derived from AIOps also improve IT decision making around operations and strategy by predicting periods of peak demand, optimising dynamic resource allocation, highlighting perpetual issues that need to be addressed, and identifying areas for cost reduction.

The value that AIOps delivers is exponentially magnified when combined with intelligent automation. By integrating these technologies, AI-driven findings can autonomously trigger automations when certain events or conditions occur. In many cases, this means that outages are avoided altogether, and in others, automation dramatically accelerates MTTR – oftentimes reducing the time required to resolve issues from hours to seconds. Together, AIOps and intelligent automation deliver a closed-loop system of discovery, detection, analysis, prediction, and automation, bringing enterprises closer to achieving the long-awaited promise of 'self-healing IT' and autonomous IT operations.

With AIOps and automation taking on much of the repetitive, task-based workload, NetOps teams can finally focus their valuable time and skills on upgrading the network to support strategic initiatives, improving end-user experience.

Hacking as a service?


Gemma Moore


Prash Somaiya


Chris Roberts


Owen Wright


Tristan Liverpool


Mark Greenwood


Ken Munro


Tom Van de Wiele


Aleksander W. Jarosz

What benefits does ethical hacking/ penetration testing provide for an enterprise?

Mark Greenwood, head of data at Netacea: "No business is required to perform penetration testing. There are plenty of willing volunteers who will be happy to do it for you. Unfortunately, those volunteers will likely steal data, commit fraud, or knock a site offline once they have access. Even if you're lucky enough to be hacked by an ethical hacker working on their own, this will start the clock on 'responsible disclosure' and may mean paying out a bug bounty. No security system should go untested, whether physical or online. Without testing, a business may have severe vulnerabilities that it simply isn't aware of, making it easy prey. Keeping up to date with patches and ensuring security best practice is followed is a great start, but on its own, it is not quite enough to guarantee peace of mind."

Chris Roberts, chief security strategist at Attivo Networks: "The term penetration testing – also known as assessment, red/purple team engagements or ethical hacking - is used to describe how an individual or team of security professionals collaborate with organisations to understand loopholes or vulnerabilities in security defences. Investigations test security from a variety of angles- from technical, human and process to procedure and control. As external, independent advisors pentesters help in-house security teams understand overall exposure to risk, appreciate organisational maturity and also help to communicate effectively across the diverse silos of data stored within the enterprise."

Gemma Moore, director at Cyberis: "Done correctly, a penetration test can highlight areas of weaknesses in your systems or applications and provide you with detailed information about the technical risks you face and how best to mitigate them. An ethical hacker or penetration tester can find weaknesses in the way your systems have been implemented and highlight how the various design and implementation decisions you have made might be abused by a range of threat actors – script kiddies, organised criminals or even malicious insiders. During a penetration test, a consultant adopts the tactics and techniques of these adversaries to demonstrate technical vulnerabilities. They can work with your technical teams to educate them, help you identify root causes of issues and give you pragmatic advice that lets you manage and mitigate the risks."

Tom Van de Wiele, principal security consultant at F-Secure: "Ethical hacking through penetration testing and related activities is used to validate the security investments that corporations have made in the form of training, technology and processes, and to ultimately make the organisation better in defending itself against cyberattacks. Although corporations perform tests on their own as part of their own due care, the focus is usually on a selected part of the organization or is constrained in other ways. Ethical hacking not only gives an attacker's view on the organisation that goes beyond these limitations, but also allows for analysis on what security investments work as expected, which ones need changing and if the incident response process matched expectations and was aligned with industry best practices. Ethical hacking also aims at helping companies shift from a pure risk based mindset towards a threat intelligence based perspective: what are attackers going to try first, where and how, and how would we be able to respond to that as defenders? The financial sector has frameworks such as CBEST, TIBER and others to aid in that process of knowing what to focus on, but for corporations in other sectors there is unfortunately still a lot of compliance based thinking."

Owen Wright, assurance director at Context Information Security: "Identify technical vulnerabilities in IT and communications systems that could leave organisations open to attack should they be exploited by a potential threat actor – from a disgruntled employee or casual hacker or a state sponsored cybercriminal. Once identified, these weak points within a network infrastructure, application or even business logic can be remediated to strengthen your overall security posture."

How do you know that your 'hacker for hire' is ethical and will work in your interests?

Tristan Liverpool, senior system engineering director at F5 Networks: "Ultimately, employing an ex-cyber-criminal is a risky decision that should be made on a case-by-case basis. It is also worth noting that criminal background checks only help identify previous offenders – they lack context on how a person has changed. For example, it is unlikely that someone charged for a denial of service attack at a young age has mutated into an international career criminal. Indeed, some young offenders often go on to become well respected security consultants and industry thought-leaders."

Aleksander W. Jarosz, threat intelligence analyst at EclecticIQ: "Competent testers will have a formal certification or formal training that will have taught them appropriate, standard operating procedures and what activity is ethical. Testers are usually required to sign off on a statement of ethical behaviour at some point in their training. This is important as a tester's certification status may be affected for acting improperly. Furthermore, any testing arrangements should involve a formal contract between the client and the testing company that spells out the nooks and crannies on what is permitted and what is not, with liabilities assigned where appropriate."

Ken Munro, security entrepreneur & industry maverick: "This is quite a pertinent question: back in 2003, a pentester working for a well-regarded firm was arrested at a trade show. It transpired that he had a past as a criminal hacker that had not been uncovered during background checks. Government security clearance is a very common requirement in pentesting roles, which can help prove that your consultant is truly ethical. Alternatives include commercial background checking processes, such as BS7858. These checks are often lacking in small pentest operations or solo operators, raising serious questions about ethical standards. That's where professional bodies such as CREST can help: they provide and verify professional standards to ensure that all accredited operators in the field operate to a high standard."

Prash Somaiya, technical program manager at HackerOne: "Ultimately, there is no incentive for a criminal to participate in hacker-powered programs, because participants are not granted any special access. Hackers benefit from remaining in good standing on the HackerOne platform. A clearly defined scope and disclosure policy, along with the HackerOne Terms & Conditions and Disclosure Guidelines, clearly outline what behaviour is authorised and what is not. Should a hacker violate any of those terms, they can be reported to HackerOne by another hacker or the impacted organisation through the platform."

What are the misconceptions about ethical hacking and penetration testing?

Chris Roberts, chief security strategist at Attivo Networks: "I would argue that the term "ethical hacking" itself is a misconception. We are simply experienced consultants who are paid to assess, review, and help organisations understand their security postures. We work in teams and have the complementary skills (physical security, electronic, internal, external social engineering, etc.) needed to carry out the assignment. The biggest misconception about hackers is failure to appreciate who we are and what we do. We're skilled and articulate. Some of us wear suits, some like to wear kilts. Most of us have a passion for what we do and for helping others. We work equally well in teams as we do alone. Most of us will blend seamlessly into your enterprise because it's part of the job. We're not social misfits, we're not outsiders, we do enjoy our hoodies but you will never catch any of us wearing gloves or masks or playing the Matrix in the background while we work. That stereotype is plain wrong but too many people still believe it."

Mark Greenwood, head of data at Netacea: "Ethical hacking is a professional industry with professional standards. It may attract a certain type of person, which is why there are schemes to tempt young people from criminal to ethical hacking, but regulations and the right accreditations mean that your data is protected and any security holes will be disclosed in a responsible manner. Pentesting is also not just about trying to break online security—many specialise in accessing physical locations, spear phishing, and checking that a site's business logic is sound."

Gemma Moore, director at Cyberis: "There's a misconception, sometimes, that penetration testers can't be trusted – there's sometimes a confusion which starts the media image of a 'hacker' in a shady basement somewhere targeting people or organisations without regard for the ethical consequences. In my experience, this is simply not true. Penetration testers tend to be extremely professional consultants and they are in the business they are in because they want to help people improve their security."

Tom Van de Wiele, principal security consultant at F-Secure: "The biggest misconceptions are usually around the tooling and the perceived model ethical hackers are operating under. Unfortunately, there are no tools or courses that will automatically change you into an ethical hacker. In the same way, an expensive kitchen knife will not automatically result in the skills and experience of a 5-star chef. Despite common misconceptions, ethical hackers have nothing in common with cyber criminals. They cannot operate without the client's written consent, they must abide by the law and bear the customer's best interests in mind at all times. That also means not doing anything that can cause physical, financial or reputational damage to the customer."

What best practices should you employ when granting access to systems to facilitate a penetration test?

Prash Somaiya, technical program manager at HackerOne: "A successful security assessment should meet two main criteria: ensuring data remains secure and leveraging people with the right skills to find vulnerabilities. Our assessments are performed by hand-picked members of our community with skills and experience that match the applications in scope. To ensure data is kept secure, it's good practice for pentesters to work with the business before, during, and after the testing period to ensure consistent feedback loops."

Owen Wright, assurance director at Context Information Security: "Agree what the scope of the test is and limit the testers access to this area of your network – apply all the normal security practices of need to know and minimum access required to do a job. The tester is likely to need high power access (eg, root, administrator or enable to the target system, but they won't need access to much else. Equally, ensure all the right commercial agreements are in place and verify the identity of your tester if they are working on your premises."

Tristan Liverpool, senior system engineering director at F5 Networks: "Like with all testing, define what you need, evaluate the skills that are required to carry out that penetration test, find out how your data will be secured and clarify the required methodology and processes. If you are going to engage with a third party to carry out the testing, get hold of a sample report to make sure it will meet with your expectations. Make sure to verify project management capabilities, ask for retest options to verify once mitigations have been put in place and most importantly, make sure liability insurance is in place in case of any impacting issues."

Gemma Moore, director at Cyberis: "Quite often, you will need to allow a penetration tester to connect to your networks with their equipment, connect to your VPNs, or you might need to create test accounts for a penetration tester, or give them access to buildings or locations. The most important thing is to make sure you have a process for documenting all access granted to the penetration tester, and a process ensuring that the access is revoked once it is not needed any more (typically at the end of an engagement). It is also best practice for a penetration test report to include a list of post-test actions that should be conducted."

What would be your best advice when hiring a penetration tester?

Ken Munro, security entrepreneur & industry maverick: "No one single pentester knows everything: it's the combination of different expertise from a team that can be brought to bear that adds real value."

Tom Van de Wiele, principal security consultant at F-Secure: "Prioritise practical experience and ability to communicate on operational, strategic and tactical levels, when setting requirements for a cyber-security company performing penetration testing. The outcome will be worth nothing unless it is communicated clearly and within the proper context. A professional penetration tester will tell you the most cost-efficient way to get the best from their time and they will choose to use their own tools. Interview the people that will be directly performing and managing the work and ask the hard questions when it comes to upholding your business continuity, how their way of working and tooling can be combined with corporate security policies and how data handling and communication should be performed from start to finish."

Gemma Moore, director at Cyberis: "The single most important feature of a successful penetration test is good communication between you and the penetration tester. Choose somebody with whom you can communicate. A good penetration tester will help you define a scope of work that will meet your needs, and answer your primary security concerns. They will make sure you understand the risks that are being identified, and will work with you and your technical teams when there are questions about what has been delivered. A good penetration tester will be flexible in what they deliver and how they deliver it to make sure they meet your needs. They will try to understand the wider context of the system in scope of attack, and try to contextualise their findings in light of the wider risks to the business. This can make a real difference in terms of realising value from a penetration test."

Mark Greenwood, head of data at Netacea: "Pentesting is like insurance: no one really wants it, but they will surely regret it if they don't do it and the worst happens. But just as important as getting it done, is getting it done regularly—far more regularly than many companies do it. Agile practices mean that businesses update their customer-facing websites and services far more often than they may have done in the past, but this means that testing is outdated far sooner than they would expect."

Chris Roberts, chief security strategist at Attivo Networks: "Two things come to mind. First, execute against the 4C's (communication, collaboration, cooperation and coordination). In-house security teams need to be your eyes, ears and understand who you are and what you need. Often, they will be your guide. Their willingness to listen, work with you and help you understand the risks along with the potential maturity discussions necessary when everything is completed will be invaluable. Second, another acronym we live by is PPT – which in this case stands for People, Process and Technology. All too often an assessment will focus on the third element and ignore the first two. All too often an assessment will focus on the third element and ignore the first two. Make sure the security assessment team you appoint can talk with you about your people and to your people. They need to understand the human and process side as well as the technology. Any fool can use exploit and assessment tools to break into your company. It's what they do with your information afterwards that separates the pentest puppy farms from the top professionals."

How can ethical hacking exercises go wrong, and how should you manage these risks?

Ken Munro, security entrepreneur & industry maverick: "By far the most common problem is a system falling over during a pentest. Systems that aren't designed to deal with unusual input can react in odd ways. Hence, it's important to ensure that your systems are well built, can fail over and the data is safely backed up. That said, outages are rare.

There's also a common tendency to blame an outage on the pentester! I remember a test a few years ago where a critical system went down, which was shortly followed by the IT director shouting furiously at us, accusing us of irresponsibly taking down their business. Only after he had said his piece could we point out that we hadn't yet connected to the network…the system wasn't fit for purpose, let alone for pentesting!"

Owen Wright, assurance director at Context Information Security: "Agree what the scope of the test is and limit the testers access to this area of your network – apply all the normal security practices of need to know and minimum access required to do a job. The tester is likely to need high power access (eg, root, administrator or enable to the target system, but they won't need access to much else. Equally, ensure all the right commercial agreements are in place and verify the identity of your tester if they are working on your premises."

Tom Van de Wiele, principal security consultant at F-Secure: "Not performing proper due diligence on both sides - customer and cyber security partner - when it comes to ownership and not adequately considering what the possible outcome could be of a certain action taken. IT environments share a lot of functionality when it comes to applications, networking and virtualisation technology. That means the dependencies from one IT eco-system in relation to another need to be understood thoroughly as certain actions taken or changes made in one might have a ripple effect towards other environments that were not included in the original scope of e.g. a penetration test. Every tool run or action taken has consequences and it is important to understand these potential consequences, being able to anticipate the risk of certain unknowns and to be able to work around them."

Aleksander W. Jarosz, threat intelligence analyst at EclecticIQ: "Not so much going wrong… but… the key to an effective penetration test is understanding and agreeing what the target and purpose of the test is. The level of assurance you require and the skill of your potential adversaries can change the recommended approach to the test. Your reasons for conducting a test will determine the approach you take. Testing for a regulatory requirement may have a well-defined set of parameters. However, testing to generally improve the security of the targeted system or overall network, or to address previously identified threats, requires more thought. Make sure your requirements are clearly defined and communicated to the test team before the test so the results are meaningful and can be utilised effectively."

DIGITAL TRANSFORMATION EXPO manchester

4-5 NOVEMBER 2020,
MANCHESTER CENTRAL

FIND OUT MORE AT DT-X.IO

Powering The Northern Tech Revolution

DTX MANCHESTER HAS BEEN POSTPONED UNTIL
4-5 NOVEMBER 2020 AT MANCHESTER CENTRAL

Overground underground

The solutions connecting the public on both rail and road

Oldest metro system gets much needed modern connections

London has the oldest Metro system in the world and TfL wanted to introduce Wi-Fi on its network to improve customer experience for the millions of people who use it every day. It was therefore the ideal choice to design and manage the deployment of Wi-Fi access across the Underground network. Fujitsu worked with partners Installation Technology to design and install a solution for ubiquitous access, Virgin Media to provide high capacity Wide Area Network connectivity, and Cisco to supply network access points compliant with the Underground environment.

The technological complexity of carrying out such a major piece of work up to 200ft underground was daunting and required highly detailed planning. Despite the difficulties, the Fujitsu team mobilised the technology in only four months to deliver the services TfL required.

In addition to the very tight deadline for completing the installation, the other major obstacle to overcome was the limited time available for work teams on a daily basis. They had access to Underground stations for only four hours a day during routine maintenance hours in the early hours of the morning. Moreover, they had to cope with working in highly confined spaces with very stringent fire regulations.

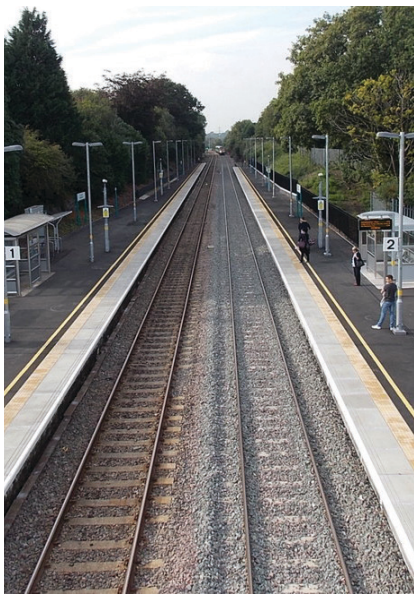
In just four months, Fujitsu designed and launched the service TfL had appointed it to deliver, enhancing the journey to work for millions of commuters. This involved installing on average 14 internet access points for each station to be Wi-Fi enabled.

In the first six months, there were over 100 million user sessions - an average of 800,000 user sessions per day. The project achieved a major milestone towards the London Mayor's goal of making London one of the world's most connected cities.

With careful planning Fujitsu were able to design, build and operate a transport communications network able to support the most challenging logistical exercise any city can undertake.

Implementing one of the first underground Wi-Fi services in Europe as required by TfL, has provided a real-time information service to enhance the journeys of customers. In addition, TfL employees are no longer tied to desk based PCs

The solution provides continuous coverage throughout each station, essential to support TfL's operational systems. The installation has been built with future requirements in mind, providing a minimum capacity of 1GB per second with in-built growth capability of Fujitsu's team performed a site analysis of every Tube station and used modelling tools to decide where the access points should be situated.



First Hull Trains get app back on track

First Hull Trains, part of FirstGroup, is a UK rail operator running 90 services a week between London King's Cross and Hull's Paragon Interchange. It carries over 800,000 passengers every year on its fleet of four Class 180 DMUs.

Its aim is to deliver an industry-leading customer experience. It has invested in and achieved various innovative industry firsts, a pioneer in the UK transport sector.

To continue this innovation, FirstGroup wanted to improve their existing app for smart devices. Through this, it would be possible to buy tickets and check train times, as before, but also to log on to station and train Wi-Fi seamlessly without the need to repeat the login process again.

In addition to these services, FirstGroup also wanted to offer all their passengers onboard media content. The successful connectivity solution needed to support all of these features.

There were five suppliers involved in the delivery of the solution, none of which had previously integrated with each other's technology.

Icomera's primary goals were to provide the onboard 4G-enabled passenger Wi-Fi and host a virtual onboard media content server while also facilitating L2 MAC authentication for Single Sign Up (SSU) between the station Wi-Fi networks and the onboard Wi-Fi.

- Virtual Onboard Media Server running on the Icomera X-Series platform
- Collaboration and integration with solution partners

Both First Group and First Hull Trains dedicated time and energy to finding a solution that would offer passengers an all-round better service. The most appropriate equipment and technologies were then selected before the installation process began.

The solution was built around the Icomera X6 router. Icomera also provided the onboard 4G-enabled passenger Wi-Fi service.

CAPMedia provided the video on demand content via a primary media server at Hull station and a virtual onboard media server hosted on the Icomera X6.

Masabi was responsible for the development of the passenger app.

Airsense created the connection management app for smart devices, handling the device authentication and handover.

DB Schenker goes the distance with SOTI

DB Schenker is one of the largest Logistics, 3PL, transport and Freight management providers worldwide, a tradition that goes back to the 19th Century (est. 1872), generating approximately 50% of the DB Group's revenues.

With more than 64,000 employees, across 130 countries and around 2,000 strategic, economic regional locations, DB Schenker has a global, integrated network geared towards customer service, quality and sustainability. A need for an enhanced mobile strategy led them to re-evaluate its enterprise mobility management solution.

As users of purpose-built handheld devices, DB Schenker realised that its current MSP platform hindered its ability to manage devices. With use of provisioning version only on Motorola devices, DB Schenker was not able to use remote control. One of its offices wanted to move from its end of life (EOL) system to a modern management system with enhanced functionality. It identified that the EOL system was cumbersome in its package build and deployment. This was compounded with the lack of remote control of devices and non-existent data collection.

Further challenges included the diverse environment (a variety of Windows Mobile, Windows Embedded Handheld and Windows CE operating systems on either 3G or Wi-Fi) and the dispersed sites. DB Schenker identified that employee enablement was limited as DB Schenker employees were reliant on external resources.

With a clear goal of improving customer satisfaction and employee enablement, the IT department had to ensure that the switch from one system to the other would not affect the day-to-day operations nor its customers' experience.

The main objective for DB Schenker was to implement a short-term seamless, integrated data management system upgrade, with the long-term benefits of speed, flexibility, greater efficiencies and overall improved customer experience.

SOTI MobiControl enabled DB Schenker to reduce the complexity of its complete device lifecycle management. With advanced helpdesk and real-time remote support the IT team was able to comprehensively manage the entire mobile deployment with ease. This improved the productivity of workers (within and outside the four walls) as well as impacted business performance.

Another key advantage that DB Schenker experienced was a lower cost of ownership because of centralized and proactive management that prompted the need to re-evaluate its enterprise mobility management provider.

By incorporating SOTI MobiControl to manage mobile deployment, DB Schenker now has access to secure, centralised information and reporting to deliver a clear competitive advantage for its customers.

Dual function Wi-Fi services for black cabs

Sherbet London Taxis, a London Black Taxi operator and advertising organisation needed to equip 50 of their latest TX4 classic Black Taxis with 4G (LTE) connectivity. The goal was to improve the experience of business customers by providing two levels of service:

1) Public internet access to customers with smart phones and tablets
2) Passenger information by means of streamed phones and tablets

There was an immediate requirement to equip 50 TX4 vehicles, followed by a further 300 vehicles during the first half of 2016 and up to 2000 vehicles over the next 5 years.

Sherbet London Taxis chose Virtual Access GW1042 router incorporating dual SIM 4G (LTE) cellular data modem, dual Ethernet ports and 802.11bgn WiFi. The FPS capability of the GW1042 was not initially required, however the ability to enable the router's GPS feature simply by changing the router's software configuration profile, was an attractive option for future cost savings. A combined cellular data and GPS antenna was included to ensure optimum access to 4G (LTE) and GPS satellite data signals.

The GW1042's ability to support multiple WiFi SSIDs means that completely separate WiFi connections are available for passenger public internet access and for in-vehicle streaming content delivery to the TFT display; the former being broadcast as public WiFi and the latter being a hidden SSID.

A key business driver for the service is to eventually enable monetisation by means of sponsorship from the clients of advertising agencies. The GlobalReach Technology captive portal solution supplied by Virtual Access enable a wide range of user analytics data to be collected and managed by cloud-based application servers. Furthermore, the technology offers the facility for gender, location and device-specific advert insertion.

Another solution differentiator was the carrier-grade Activator router provisioning and monitoring system designed to scale to tens of thousands of devices. This technology removes the need for routers to be pre-configured, so they can be installed without staff skilled in networking. This enabled Sherbet London Taxis to benefit from rapid deployment as well as the ability to centrally manage router configuration changes and updates if needed.

Smarter farming

How farmers are using the Internet of Things to improve produce quality

Smart agriculture and organic farming are two trends strongly linked. In the United Kingdom are walking hand in hand for a while to improve competitiveness of small producers. Senseye, a UK software company focused on prognostics and conditions monitoring, decided to develop a project with organic farmers to increase their crops and make them sustainable.

Since the beginning, the Senseye engineer team detected a lack of freely available public data in matter of agriculture issues, so they decided that it was necessary to work elbow to elbow with farmers and deploy a sensor network around the country to collect data.

This project was deployed in nine farms located across the UK, from Riverford Organic Farms in Devon to Spen Farms run by the University of Leeds. The aim of this project was to be able to capture useful data to start predicting measurements and events that could help farmers and agronomists to save time and money with its farms. In this project, it has been deployed in a diverse range of crops, from vegetables to grain.

There was not any similar project so the system deployed was built from the ground-up. Besides, there were some 'musts' that defined the project. First of all, the solution must have a competitive price. Besides, the devices should be easy to setup and, of course, with low maintenance costs. Finally, the systems should have the ability to send data to Senseye cloud service with a minimal fuss. Libelium devices were chosen because of some reasons:
The best comparative price and value for money.

- All the sensors were integrated and available.
- The API and the codebase.
- The Waspmote Plug & Sense! Sensor Platform 'ready out of the box' idea.

In this case, Senseye chose Waspmote Plug & Sense! Sensor Platform, fully equipped with Libelium sensors, because of its features of automatic functioning, high resistance, durability and easy implementation. In fact, one of the experts involved in the project, Joe Britto, highlights these features about Libelium products: "We managed to install each unit on average in about 20 minutes". Specifically the devices installed were the following:

- Five Waspmote Plug & Sense! Smart Agriculture PRO, with Digital Humidity & Temperature probe, Soil temperature probe, Solar radiation probe and Soil moisture probe.
- Twelve Waspmote Plug & Sense Smart Agriculture, with Digital Humidity & Temperature probe, Soil moisture probe, Soil temperature probe and Weather Station WS-3000 probe
- Four Waspmote Plug & Sense Smart Environment, with NO2 probe, NH3 probe, CO2 probe, Temperature probe, Humidity probe and Volatile Organic Components sensor probe.

The devices communicated directly to the Senseye cloud by GPRS communication protocol. Besides, in spite of its prolonged battery life, the nodes were equipped with a solar panel to ensure a long life and an autonomous functioning.

These nodes were used to monitor a wide range of environmental issues that affect directly to agriculture, for example solar radiation, wind speed and direction, rainfall, ambient temperature, humidity, gases, VOCs, soil moisture and temperature.

This project set the foundations of active projects in the future because the predictions and warnings about agriculture events can be useful for optimizing crop yields and therefore saving time and money to the agriculture business owners. "The system we developed was to predict parameters that would have effects on crop growth – so that farmers could be warned about threats to their yield", affirms Alexander Hill, co-founder of Senseye. Some parameters such as poor weather conditions or likelihood of pest infestation or disease could be prevented thanks to the sensors. The project was successful in that data was enough to predict matters like this accurately.

This deployment was a research-focused project to gather data and develop prediction models in matter of, for example, crops yield or adverse conditions. Farm owners and managers were impressed by the amount of measurements that could be taken and how capable the sensors were. They also feel relaxed during the sensors installation in the fields because they were quick and simple deployments with huge possibilities for their daily work.

This project was deployed in nine farms across the UK, from Riverford Organic Farms in Devon to Spen Farms run by the University of Leeds

MooCall connecting man with animal

The idea for the MooCall calving sensor came about when one of the MooCall founding team, Niall Austin lost a heifer and her calf due to a difficult calving back in 2010. He had a theory that a device to measure tail movement might be able to predict the onset of calving and brought the idea to the other MooCall founders Michael Stanley and Emmet Savage. After many months of research and development the MooCall device was born, however they needed robust and reliable, global connectivity with roaming capability to ensure that this critical data could be transferred the crucial moment. Vodafone IoT worked closely with MooCall to implement a solution that works seamlessly every time, wherever the cow might be situated.

This non-invasive, tail mounted sensor gathers over 600 pieces of data a second. It can accurately predict when a cow is most likely to give birth by measuring tail movement patterns triggered by labour contractions. When they reach a certain level of intensity over a period of time it then sends an alert, via the Vodafone Managed IoT Connectivity Platform, directly to your cell phone or via an app, on average one hour prior to calving.

"Vodafone IoT gives us the roaming capability to get our signal out whatever the location," said Emmet Savage,CEO MooCall. "We have a huge expansion plan and in every case whichever country we've signed agreements in Vodafone IoT has their IoT Platforms in those jurisdictions so it makes the globalisation of MooCall seamless."

The fundamentals in the pursuit of agility: a backbone for success

Paul Ruelas, senior director product management, GTT

Agility is a key when considering a business's competitive edge, but how do we define it? With many businesses using the phrase interchangeably with speed, productivity and adaptability - what does it really mean?

First and foremost, agility is becoming synonymous with digital transformation and is the latest IT industry buzzword. When it comes to understanding the difference between agile development and agile practices, the definition is easier to get to grips with. Yet, it's important to understand that the two go hand-in-hand when thinking in the context of networking.

As businesses continue to focus on digital transformation, they become dependent on the underlying network that aids their business processes, productivity and outputs. For example, an enterprise may choose to run sprints and stand-up meetings to drive quicker competitive advantage. However, this can be hindered if its cloud networking infrastructure isn't able to ensure that rapid and continuous updates can be deployed to the business. Likewise, as businesses become more reliant on agile cloud-based applications, they must ensure consistent application performance to provide a seamless user experience. That all relies on a robust underlying network.

To really gain first-mover advantage and be an industry leader, businesses need the ability to pivot and adjust as markets, customer demands, and business models dictate. Firstly, businesses need to ensure that the network is application aware, predictable, accessible and cloud integrated. Applications are now distributed across IT environments - some living in the data centre, some at the edge and some in the cloud. This means organisations need the ability to connect to and access any application regardless of its location. An application-aware network can identify and classify applications and apply the appropriate optimisation to ensure peak performance per user.

In a digital economy there is little room for sub-optimal performance of applications as businesses, employees and customers expect a consistently smooth and seamless experience, even when using a cloud network. This means that secure network connectivity needs to encompass the cloud to offer greater flexibility, agility and scalability. In addition, organisations should be able to ensure sustained availability of the network by leveraging the ability to have two or more lines in operation as a precautionary solution for failover.

Secondly, it is undeniable that to enable agility, the network needs to be flexible, available on demand and easy to manage. Organisations need the ability to make real-time changes to user access or bandwidth to either support specific projects, or to support a spike in employee workload for a short duration.

Similarly, the organisation needs the ability to provision changes. With automated policy management, organisations have the ability to automatically roll-out changes or updates to the enterprise network at speed, regardless of location.

To make this agile elysium a reality, organisations need to consider how they can re-architect their network for a digital age. Agility is all about enabling enterprises to pivot quickly in response to change – potentially requiring the introduction of new products or services, the need to enter a new market or even create a new digital-centric business model.

In the coming years, software defined wide area networking technologies (SD-WAN) is well positioned to become a strategic enabler for companies, allowing them to increase efficiency, enhance performance and improve security without increasing costs. SD-WAN offers the promise of zero-touch provisioning, allowing for faster time of service deployment. The availability of SD-WAN with universal CPE also creates the possibility of service chaining, providing the ability seamlessly add networking functionality such as WAN optimization and enhanced security without the time and expense of deploying additional hardware. By prioritising a new networking approach, organisations can effectively prepare for the future and preserve their competitive edge.

With more and more businesses across sectors and geographies digitising their offerings, it's time to embrace SD-WAN to support a cloud-based future, and gain the agility required of a digital world. It offers businesses enhanced control of their network, improves visibility, and supports performance while offering bandwidth efficiency - all without increasing costs.

When moving to SD-WAN, it's important to look for features that simplify network management. Offerings that allow businesses to use a single device to connect to multiple functions, manage software updates all in one place, reduce hardware costs and simplify installations, will consolidate network functions. In turn, this will improve agility and make it easier to roll-out new networking services.

Thinking about SD-WAN? Here's how to buy only what you really need

Sylvain Quartier, VP of marketing and product strategy, Ekinops

SD-WAN has emerged as compelling to satisfy demands for a highly evolved network. Yet, like any significant upgrade, SD-WAN brings adoption challenges and costs. You need to consider both in making your choice.

What's more, as the market has become saturated, "the right path" to SD-WAN has become harder to identify. So, when time and resources are stretched, is there a best practice formula? Sadly not; there is no "one-size-fits-all".

That said, there are factors that should contribute to your SD-WAN adoption strategy to get you off to a good start.

Love your legacy? Extending your MPLS system does not offer the flexibility and agility you need. Put simply, you need SD-WAN. But does that mean it's time to clear out your legacy services?

Not quite. Service providers see an opportunity to tap-in to new revenues by offering SD-WAN as a managed service.

After all, many users are not asking to get rid of their MPLS services. Rather, they are asking how they can get greater agility and control over their application traffic management and cloud access.

A managed SD-WAN also reduces the time and resources you need to spend.

Keep it simple Deployment and maintenance should be low cost and as easy as possible. The cost of launching a managed SD-WAN is mainly operational, rather than related to technology. Zero-touch provisioning is invaluable, saving time, cost and technical complexities associated with site intervention.

While "off-the-shelf" SD-WANs have commonly required additional hardware, new products that use existing hardware – or added as an extension – are now changing the market. With SD-WAN as one of a number of functions within a single box, both management requirements and costs can be dramatically reduced.

Open up to new ideas Selecting an SD-WAN based on its openness can be a game changer and will protect your investment in the longer-term. Vendor lock-in not only leads to higher pricing, it also restricts innovation.

With an open solution, integrating new services from third parties is not only possible, it's very plausible. It can still support those "big brand" services if that's what you require.

Pay for what you need and nothing more Many off-the-shelf products deliver far more than is actually ever required, needlessly increasing TCO.

A small- or medium-sized business simply trying to extend its network with local break-out doesn't need the same SD-WAN as a large enterprise with business-critical applications to protect.

Develop clear projections for the applications and likely capacity you'll need. This should go some way to highlighting the benefits of opting for a modular offering from a smaller specialist, instead of buying by default from the big brands.

As well as promoting cost-efficiency, this is also a brilliant way to ensure your chosen SD-WAN is flexible and future-proof. And you can scale up in response to future new requirements.

New features have been added by **Aruba** to its SD-Branch product, part of the company's edge-to-cloud strategy.

SD-Branch integrates the company's Branch Gateways with its Central cloud management. This, says Aruba, provides a single point of control and management for SD-WAN, wired and wireless networking for secure, simplified branch connectivity.

Features added include expanding branch defence to provide identity-based attack detection and intrusion prevention.

This includes: one-click integration with cloud-based security solutions; threat visibility and trend analysis; correlation of security events with sites, clients, applications and infrastructure; policies for enforcement and incident response; security event streaming to third-party security and event management products; and ClearPass Policy Manager.

Other features are enhancements to edge-to-cloud management and secure connectivity; and gateways for non-stop connectivity via built-in cellular, including LTE.

Aruba, owned by HPE, says SD-Branch is ideally suited to retailers with large distributed networks.

The Truffle-EX series software defined WAN orchestration and broadband bonding appliance, enables cost-effective and self-healing internet access for businesses, enterprise branch offices and other multi-tenant buildings.

Designed specifically for large offices and data centres, Truffle EXX is a new version of **Mushroom Networks**' Truffle broadband bonding SD-WAN devices.

It is designed to support up to 26 ports with configurable NIC modules with fibre and/or copper ports as 1Gb and/or 10Gb Ethernet.

Mushroom says Truffle EXX supports its latest SD-WAN software and offers near wire-speed performance for the overlay tunnels.

Measuring 430x475x44mm, the unit has 18 configurable WAN and eight built-in LAN ports in a 1U rack-mountable form factor.

Mushroom says it sees SD-WAN 10Gb capacity becoming more commonplace with big companies and service providers.

Like the company's other SD-WAN models, it is said to leverage automated overlay tunnels that can detect flow types, analyse transport metrics in real-time and so apply flow specific algorithms to optimise application performance. Network automation enables hands-off network management.

Four "as a service" products have been added by **Aryaka** to its newly-branded SmartServices SD-WAN range.

They comprise SmartConnect, connectivity as-a-service with global and new regional offers, last mile and HybridWAN; SmartOptimize, network and application acceleration featuring TurboNet and TurboApp; SmartCloud, managed multi-cloud networking for public clouds, SaaS providers and partner clouds; SmartSecure, including managed firewall and network function virtualisation for pureplay firewall products; and SmartInsights, using cloud-based MyAryaka.

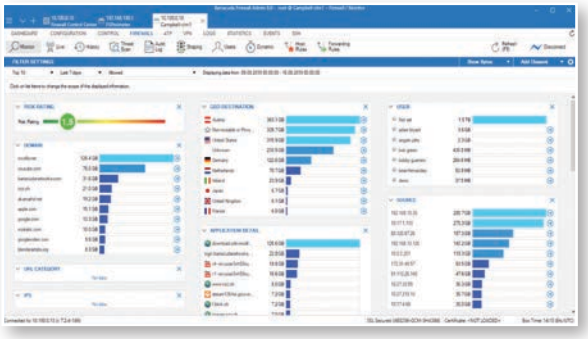
All are managed, orchestrated and monitored globally by the company's SmartManage service.

Aryaka says it is now making its premier global SD-WAN offering available – with the same quality – for "regional" deployments using pre-defined regional clusters and points-of-presence. And users can upgrade to a global SD-WAN service with no disruption.

Aryaka says it is well positioned to differentiate itself and disrupt "do-it-yourself" box vendors as well as traditional service providers.

In a new release of CloudGen Firewall, **Barracuda Networks** says it has added functions to help streamline SD-WAN management, optimise cloud connectivity and automate scalable protection across multi-cloud deployments.

Barracuda says many rival SD-WAN products require days to deploy and can introduce vulnerabilities if not correctly configured.



CloudGen Firewall, it says, provides an all-in-one SD-WAN solution that is integrated with public cloud infrastructure, giving users security and connectivity and automation to make their lives easier.

It says Release 8 adds a range of automation features to streamline deployment and provide visibility and control for successful implementations.

In addition, the company says that in extending the capabilities of Firewall Insights, the new "WAN Patch Controller dashboard" dynamically displays global SD-WAN data on network and remote location health status, so users can make more efficient use of WAN resources while improving performance.

SD-WAN users can offload network and security configuration and change management says **Cato Networks** in introducing Hands-Free Management.

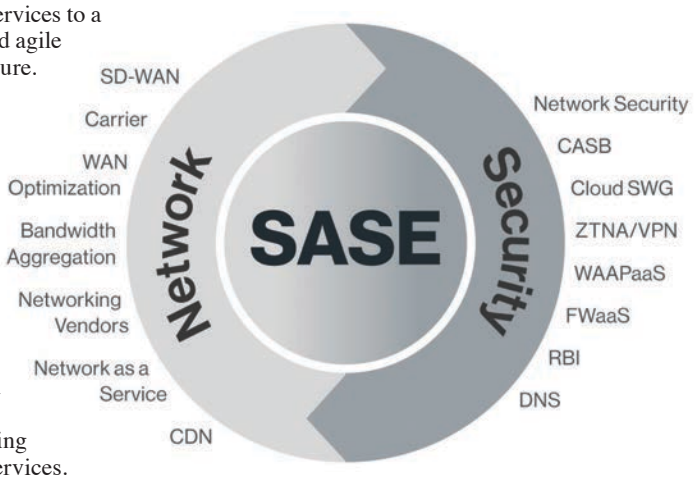
At the same time, users can retain control of networks through self-service and co-management already included in Cato Cloud

In addition, Cato Managed Services includes: managed threat detection and response which continuously monitors the network; intelligent last-mile management; and rapid site deployment assistance.

Cato says it offers the world's first SASE (Secure Access Service Edge) platform, uniting SD-WAN and security into a global cloud-native service.

This, it says, enables businesses to move from "rigid and expensive" MPLS and costly managed services to a unified, secure and agile network architecture.

The benefits, says Cato, include: easy migration from MPLS to SD-WAN; improved performance; direct and secure internet access to branches and mobile users; and access from anywhere without using premium cloud services.



Please meet...

Matthew Pincus is the managing director, EMEA and India at AddOn Networks, part of the Halo Technology Group. Networking+ caught up with him to talk about his life away from the workplace

What is the best thing about your job?

I know it's the 'wrong' answer, but the best thing about my job is going home at the end of the day. I enjoy my job, but I love the look on the face of my 1-year old when I walk in the door, and I'm happy that what I do provides for her.

Within my job? It's building. When I joined AddOn it was a very small business, with very manual processes. In the years since, we've built systems – our production and quality management system, our content database, a bespoke CRM – that enable us to be self-sustaining and grow. I'm never not busy, but to devote a month to building a system, taking a holiday and then coming back to see it thriving is very satisfying.

Who has been your biggest inspiration?

My closest friends: I've only ever been as ambitious as my peer group. I'm satisfied with what I've achieved so far but, for instance, a close friend recently took a senior position at Google and it raised the bar for our whole group; maybe he felt the same when I took a leadership role. We all support each other, but there is a friendly competition that drives us all. I think a strong support network is an incredibly important part of anyone's personal development; the people who you surround yourself with should always be an encouraging force.

What is your biggest regret?

I wish I could go back and relive being 15-25. I was young and stupid, as you'd expect from a teenager, but to do it again with just a bit more maturity and direction would have opened up so many opportunities for me earlier on. Instead, I coasted and have spent my 30s trying to catch up. Whilst I am grateful for my position now, I wish I could tell my younger self that there is no easy way up, but it can be made easier by adopting some ambition.

If you had to work in a different industry, what would it be?

Definitely sports. I was never very athletic, but I loved playing regardless, as well as reading the scores and stats in the newspaper every morning. Every major sport has been transformed by data analytics in the past 20 years to optimize performance and it's fascinating to see how that envelope is continually pushed. The merger of industries which are so different, coming together to boost the performance and instigate the evolution of one another, is fascinating. Perhaps now, my skills wouldn't be so out of place in the athletic field after all!

Who was your hero when you were growing up?

My mom was a single mother who not only made sure I was taken care of – safe, fed, educated – but that I had opportunities to explore – to travel, to try new things – even when money was tight. She's a hero for all the obvious reasons, but the most valuable lesson that I have to thank her for is the sense that, no matter how things look today, anything is possible tomorrow. This mindset that she has granted me with is one that has been very valuable throughout my life, and one that I hope to instill into my daughter, as she did to me.

The Beatles or the Rolling Stones?

The Beatles. Both are before my time and both certainly have tons of songs I know, but people make the argument for the Rolling Stones by comparing them against the Beatles when, the fact is, the Beatles stand on their own. The Rolling Stones have longevity, but history will only remember their respective peaks, whereas The Beatles are ubiquitous.

What would you do with £1m?

Firstly, convince my wife we should take an overly lavish vacation! Then, probably invest most of it. However, I would definitely be aggressive and a bit risky with the investment – maybe a big investment in some Bitcoin start-up?

Which rival do you most admire?

Fiberstore. They're not exactly a rival and, as with any company, they have their share of flaws, but I love the efficiency of their operation. They're built to scale and they're doing it well. By combining the best parts of their organisation with the best parts of ours, we could dominate the industry.

What's the weirdest question you've been asked at an interview?

It was a job interview question, but it's weird enough to stand out in any context: You're given an elephant that you can't give away or sell. What do you do with it?

If you could change any UK law, what would it be?

Brexit. As an American expat and impassioned traveller, I want to see borders melt away. I admit I don't know all of the politics and history, but it feels like a step backwards in global fluidity and union. In my ideal world, free movement would be a given; such encouragement and facilitation of worldwide diversity can only enrich our cultures and help us learn from one another, rather than divide us.

aryaka

The Cloud-First WAN Company

Aryaka, the Cloud-First WAN company, brings agility, simplicity and a great experience to consuming the WAN-as-a-service. An optimized global network and innovative technology stack delivers the industry's #1 managed SD-WAN service and sets the gold standard for application performance. Aryaka's SmartServices offer connectivity, application acceleration, security, cloud networking and insights leveraging global orchestration and provisioning. The company's customers include hundreds of global enterprises including several in the Fortune 100.

Fully Managed SD-WAN Service

> "...A quick note regarding Coronavirus to let you know we're in great shape thanks to the foundations we've laid down on both the core network and WAN with Aryaka. We've got multiple options to enable staff to work from home and use best of breed cloud services. It's also great to have a lot of visibility across the network and headroom to scale as needed."

Richard Delisser,
VP of Global Infrastructure,
World Fuel Services

> "I would like to mention to you and everyone [at Aryaka] that the best decision we could have made as a customer was the implementation of Aryaka. The impact it has made to quickly move from an on-site office environment to a near 100% virtual/remote office scenario has been, in my opinion, the difference in success vs. failure. Keep up the great work and I hope everyone remains safe throughout this new reality."

Mark Baker,
CTO, Pilot Freight Services